

### REMARKS

After entry of the foregoing amendment, claims 29-56 are pending in the application. Claims 1-28 have been canceled, but their subject matter has been reintroduced in the new claims.

Although the new claims are broader in certain respects than the canceled claims, each of the new claims is believed to be patentable over the art of record.

For example, each of claims 1-28 was rejected as anticipated by, or obvious in view of, Borza (5,995,630).

Borza is understood to disclose a video contact imager, including a CCD,<sup>1</sup> that serves to image a person's finger using prism optics and thereby obtain a fingerprint image. (Borza's fingerprint-capturing contact imager is shown at block 120a in Fig. 4b.<sup>2</sup>) This image is matched against a collection of previously-stored fingerprint data to identify the user. Once the user is thereby identified, the system looks up a particular cryptographic key corresponding to that user. Data files stored by the user can then be encrypted with that key, and files accessed by the user can be decrypted with that key.

In the Borza passages particularly cited by the Examiner, the encryption key is sent to the user by encoding the key into a frame of video data, by substituting bits of the cryptographic key for the least significant bits of video pixel data, at locations around the margins of the video frame.<sup>3</sup> This arrangement for key transmission is used to help avoid detection. The video data in which this pixel-substitution procedure is performed is the image of the person's finger.

New method claim 29 specifies that the base data into which the claimed operator attribute data is encoded, is captured "from a subject distinct from the operator." This is exactly the opposite of Borza, who encodes data into a video image of a fingerprint. A fingerprint is not "a subject distinct from the operator." Rather, the subject of Borza's image is the operator.

This distinction is shown in Fig. 2. Two distinct images are captured in the illustrated embodiment: the user's eye at the left side of the illustration ("Image source 1"), and a landscape scene at the right side of the illustration ("Image source 2").

New claim 48 calls for a digital camera having an optical system for imaging a subject

---

<sup>1</sup> Claim 8; col. 11, lines 34-40.

<sup>2</sup> Col. 9, lines 4-5.

onto a photosensor array, and a capture system for capturing biometric information associated with an operator of the camera. The claim requires that the capture system include one or more elements in addition to said optical system. If Borza is compared to claim 48, it will be recognized that his biometric capture system includes no element in addition to his video (subject) capture system. This is because the subject Borza's arrangement is designed to capture is the fingerprint image, alone.

This distinction is also shown by applicant's Fig. 2. The attribute capture system includes, e.g., an eyepiece, and an optical element 204 that directs light reflected from the operator's eye onto the CCD 208. Neither this eyepiece nor this optical element 204 is used in imaging the camera subject (i.e., the landscape scene shown in the right side of Fig. 2) onto the CCD. Again, in Borza, only a single image is captured, so only a single set of capture system elements is provided.

New claim 49 is a method claim in which identification data is decoded from the received content data. Unlike Borza, the claimed identification data comprises biometric information captured from an operator of equipment that originally captured said electronic content, which biometric information has been algorithmically processed to yield a more compact representation. It will be recognized that the data conveyed in Borza is a cryptographic key that was associated (e.g., through a table look-up operation) with the fingerprint data. No series of mathematical operations can transform Borza's fingerprint data into his cryptographic key data; they appear wholly independent. His cryptographic key data thus does not meet the claim requirement of "biometric information ... which has been algorithmically processed to yield a more compact representation."

Moreover, claim 49 further requires "checking said decoded identification data for correspondence with reference data." It will be recognized that Borza – upon decoding the cryptographic key from the video signal – does not check it for correspondence with reference data. Rather, Borza teaches that the key is directly used, for file encryption and decryption. No comparison or check is contemplated.

The dependent claims further distinguish the art.

The other cited references have been reviewed, and they are not believed to suggest to an

---

<sup>3</sup> Col. 1, lines 1-10.

artisan that Borza be modified in the radical ways necessary to yield the claimed arrangements. Schwartz (5,767,496), for example, discloses encoding retinal data in bar code printed on a credit card. He does not suggest capturing retinal data in a device or method that captures, e.g., a photograph or a sound recording. Only through impermissible hindsight can Schwartz's retinal data teachings be isolated from his primary focus on credit cards, and applied in the context of media capture arrangements like those claimed.

The new claims have been carefully drafted, bearing in mind guidance received in the previous four rejections. The pending claims are believed well suited for issuance, and action to that end is solicited. The Examiner is invited to telephone the undersigned if any issue remains.

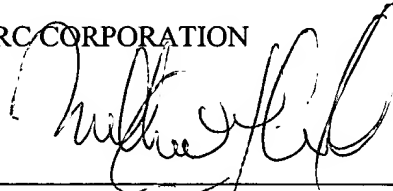
Date: December 13, 2004

**Customer Number 23735**

Telephone: 503-885-9699  
FAX: 503-885-9880

Respectfully submitted,

DIGIMARC CORPORATION



By \_\_\_\_\_

William Y. Conwell  
Registration No. 31,943